

IN THE CLAIMS

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Currently Amended) A method for a provider of software to authenticate users of the software, comprising the steps of:

constructing a puzzle in response to information received from a user, the puzzle including the information, wherein the constructing step comprises the steps of deriving a value from the information to produce a derived value, exponentiating the derived value to produce an exponentiated value, and combining the exponentiated value with a portion of the derived value;

sending the puzzle to the user;

returning a solution to the puzzle to the provider;

~~The method of claim 4, further comprising the steps of~~

storing the information and a random number[[],] ;

performing a hash function on the information and the random number to generate a first hash result[[],] ; and

encrypting the first hash result[[],] ;

wherein the deriving step comprises the steps of partitioning the encrypted hash result into first and second components, performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the derived value.

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Cancelled)

11. (Currently Amended) An apparatus for enabling a provider of software to authenticate users of the software, comprising:

means for constructing a puzzle in response to information received from a user, the puzzle including the information; ~~The apparatus of claim 7, wherein the means for constructing a puzzle~~ further comprises means for deriving a value from the information to produce a derived value, means for exponentiating the derived value to produce an exponentiated value, and means for combining the exponentiated value with a portion of the derived value[.];

means for sending the puzzle to the user; and

means for returning a solution to the puzzle to the provider;

~~The apparatus of claim 10, further comprising~~ means for storing the information and a random number;

means for performing a hash function on the information and the random number to generate a first hash result[.]; and

means for encrypting the first hash result[.];

wherein the means for deriving means for partitioning the encrypted hash result into first and second components, performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the derived value.

12. (Cancelled)

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) An apparatus for enabling a provider of software to authenticate users of the software, comprising:

a processor; and

a processor-readable storage medium accessible by the processor and containing a set of instructions executable by the processor to construct a puzzle in response to information received from a user, the puzzle including the information, and sending the puzzle to the user;

The apparatus of claim 13, wherein the puzzle is constructed by deriving a value from the information to produce a derived value, exponentiating the derived value to produce an exponentiated value, and combining the exponentiated value with a portion of the derived value; and

The apparatus of claim 16, wherein the set of instructions is further executable by the processor to store the information and a random number, perform a hash function on the information and the random number to generate a first hash result, and encrypt the first hash result, wherein the derived value is derived by partitioning the encrypted hash result into first and second components, performing a hash function on a concatenation of the first component and the random number to generate a second hash result, appending a plurality of zero values to the second component to produce a lengthened second component, performing an exclusive-OR operation between the lengthened second component and the second hash result to generate an exclusive-OR result, and concatenating the first component and the exclusive-OR result to produce the derived value.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)